View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

ACADEMIC PRESS

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Algebra 257 (2002) 222–243

JOURNAL OF Algebra

www.academicpress.com

Sastry automorphisms

E. Bombieri

Institute for Advanced Study, Princeton, NJ 08540, USA

Received 1 March 2002

Communicated by Michel Broué

Dedicated to J.G. Thompson on his 70th birthday

1. Introduction and results

Some time ago, N.S.N. Sastry [S] studied the question of the uniqueness of the embedding of the Ree groups ${}^2F_4$ in the untwisted groups F_4 over a field of characteristic 2. This led him to the problem of characterizing all automorphisms f of a field k of characteristic 2, with the following property:

There are elements $z = (z_1, z_2, z_3, z_4)$ *in* $(k^*)^4$ *such that*:

$$z_1 = (z_1 z_2)^f; \tag{1}$$

$$z_1 z_2^{-1} z_3 z_4 = (z_2 z_3)^{2f} \quad \text{or} \tag{2I}$$

$$z_1 z_2 z_3^{-1} z_4^{-1} = (z_2 z_3)^{2f}; \tag{2II}$$

$$\begin{aligned}&\big(1 + (z_1 z_2^{-1} z_3^{-1} z_4)^m\big)\big(1 + (z_2 z_4^{-1})^m\big)\big(1 + z_3^m\big)\\ &\quad = \big(1 + (z_1 z_2^{-1} z_3^{-1} z_4)^{mf}\big)\big(1 + (z_2 z_4^{-1})^{2mf}\big)\big(1 + (z_3 z_4)^{mf}\big),\end{aligned} \tag{3m}$$

$$\begin{aligned}&\big(1 + z_4^m\big)^3\big(1 + (z_2 z_3^{-1})^m\big)\big(1 + (z_3 z_4^{-1})^{2m}\big)\big(1 + (z_1 z_2^{-1} z_3^{-1} z_4^{-1})^m\big)\\ &\quad = \big(1 + z_4^{4mf}\big)\big(1 + (z_2 z_3^{-1})^{2mf}\big)\big(1 + (z_3 z_4^{-1})^{mf}\big)^3\\ &\qquad \times \big(1 + (z_1 z_2^{-1} z_3^{-1} z_4^{-1})^{mf}\big)\end{aligned} \tag{4m}$$

for $m = 1, 2, 3, \ldots$.

We shall refer to such an automorphism as a *Sastry automorphism*.

E-mail address: eb@math.ias.edu.

0021-8693/02/$ – see front matter © 2002 Elsevier Science (USA). All rights reserved.
PII: S0021-8693(02)00518-5

A correspondence with Sastry ensued, which eventually led to the solution.

The elimination of variables used is reminiscent of certain ideas which occur in the characterization of the Thompson automorphisms arising in the problem of uniqueness of the twisted Ree groups ${}^2G_2$, see [T,B,E]. Thus, even if the embedding problem in the meantime may have been solved by less computational methods,[1] it may be not inappropriate to present the result of this research here in an article dedicated to John Thompson.

We note that we can always restrict k to the subfield $k_0 = \mathbb{F}_2(z)$ generated by the z_i's over the field $\mathbb{F}_2$ of 2 elements. We say that a Sastry automorphism is of Type I or II according to whether (2I) or (2II) holds.

It turns out that there are 22 families of solutions and 22 sporadic solutions over small finite fields, the largest of which is the Galois field $\mathbb{F}_{2^{10}}$.

Theorem. *Tables* 1 *and* 2 *gives a complete list of Sastry automorphisms for the action on the field* $k_0 = \mathbb{F}_2(z)$*, described in terms of parameters* $x = z_1/z_3$ *and* $y = z_3$ (*and* y *alone whenever possible*).

Table 1

Type I	z			
(I, Ai)	$(y^{2-f}, y^{1-f}, y, 1)$	$y^{(f-1)^2} = 1$		
(I, Aii)	$(y^{2-2f}, y^{2-2f}, y, y)$	$y^{(f-1)(2f-1)} = 1$		
(I, Aiii)	$(xy, y, y, x^{-1}y)$	$x^{f-1} = 1$, $y^{2f-1} = 1$		
(I, Aiv)	$(y^{-3+4f}, y^{-2+2f}, y, y^{-2+2f})$,	$y^{(f-1)(2f-1)} = 1$		
(I, Av)	$(y^{-1+2f}, 1, y, 1)$	$y^{(f-1)(2f-1)} = 1$		
(I, Avi)	(y^{-1+4f}, y, y, y)	$y^{(2f-1)^2} = 1$		
(I, Avii)	$(xy, x^{2f-1}, y, 1)$	$x^{2f^2-1} = 1$, $y^{f-1} = 1$		
(I, Aviii)	$(xy, x^{2f-1}y, y, y)$	$x^{2f^2-1} = 1$, $y^{2f-1} = 1$		
(I, Aix)	$(xy, (xy)^{-1+2f}, y, y^{-1+2f})$	$x^{2f^2-1} = 1$, $y^{2f^2-1} = 1$		
(I, Ax)	$(y^{3+2f-4f^2}, y^{2-2f^2}, y, y^{2f-2f^2})$	$y^{(f-1)(2f^2-1)} = 1$		
(I, Axi)	$(y^{-1+2f+4f^2}, y, y, y^{1+2f-4f^2})$	$y^{(2f-1)(2f^2-1)} = 1$		
(I, Axii)	$(y^2, 1, y, y^2)$	$y^3 = 1$	$f = 1$,	$k_0 = \mathbb{F}_{2^2}$
(I, Axiii)	(y, y^2, y, y^2)	$y^5 = 1$,	$f = 2$,	$k_0 = \mathbb{F}_{2^4}$
(I, Axiv)	(y, y^3, y, y^3)	$y^5 = 1$,	$f = 2^2$,	$k_0 = \mathbb{F}_{2^4}$
(I, Axv)	$(y^5, 1, y, y^3)$	$y^7 = 1$,	$f = 1$,	$k_0 = \mathbb{F}_{2^3}$
(I, Axvi)	$(y^3, 1, y, y^5)$	$y^7 = 1$,	$f = 1$,	$k_0 = \mathbb{F}_{2^3}$
(I, Axvii)	(y, y^4, y, y^4)	$y^9 = 1$,	$f = 2$,	$k_0 = \mathbb{F}_{2^4}$
(I, Axviii)	(y, y^3, y, y^3)	$y^9 = 1$,	$f = 2^4$,	$k_0 = \mathbb{F}_{2^4}$
(I, Axix)	$(x, x, 1, x)$	$x^3 = 1$,	$f = 2$,	$k_0 = \mathbb{F}_{2^2}$
(I, Axx)	(y^3, y^3, y, y^3)	$y^7 = 1$,	$f = 2^2$,	$k_0 = \mathbb{F}_{2^3}$
(I, Axxi)	(y^4, y^4, y, y^4)	$y^7 = 1$,	$f = 2^2$,	$k_0 = \mathbb{F}_{2^3}$
(I, Bi)	$(y^6, 1, y, y)$	$y^9 = 1$,	$f = 2^2$,	$k_0 = \mathbb{F}_{2^6}$
(I, Bii)	$(y^3, y^3, y, 1)$	$y^9 = 1$,	$f = 2^3$,	$k_0 = \mathbb{F}_{2^6}$

[1] The author has been unable to find a reference to a published work on this embedding problem.

Table 2

Type II	z			
(II, Ai)	$(y^{1+2f}, 1, y, 1)$	$y^{(f-1)(2f+1)}=1$		
(II, Aii)	$(y^{3+4f}, y^{1+2f}, y, y^{1+2f})$	$y^{2f^2-1}=1$		
(II, Aiii)	(y^{1+4f}, y, y, y)	$y^{4f^2-2f-1}=1$		
(II, Aiv)	$(y^{2+f}, y^{1+f}, y, 1)$	$y^{f^2+f-1}=1$		
(II, Av)	$(y^{1+2f}, y, y, y^{1-2f})$	$y^{2f^2-1}=1$		
(II, Avi)	$(y^{2+2f}, y^{2+2f}, y, y)$	$y^{(f+1)(2f-1)}=1$		
(II, Avii)	$(y^{2+2f}, y^{2f}, y, y^{-1+2f})$	$y^{2f^2-1}=1$		
(II, Aviii)	$(y^{1+f+2f^2}, y^{f}, y, 1)$	$y^{2f^3-1}=1$		
(II, Aix)	$(y^{\frac{3}{2}+2f+2f^2}, y^{\frac{1}{2}+\frac{3}{2}f+f^2}, y, y^{\frac{1}{2}f+f^2})$	$y^{2f^3+f^2-1}=1$		
(II, Ax)	$(y^{1+2f+4f^2}, y^{1+2f}, y, y)$	$y^{4f^3-1}=1$		
(II, Axi)	$(y^{\frac{1}{2}+2f+2f^2}, y, y, y^{\frac{1}{2}-2f+2f^2})$	$y^{4f^3-f-1}=1$		
(II, Axii)	$(x, x, 1, x)$	$x^3=1,$	$f=2,$	$k_0=\mathbb{F}_{2^2}$
(II, Axiii)	(y^2, y^3, y, y^3)	$y^{11}=1,$	$f=2^7,$	$k_0=\mathbb{F}_{2^{10}}$
(II, Axiv)	$(1, 1, y, y)$	$y^3=1,$	$f=2,$	$k_0=\mathbb{F}_{2^2}$
(II, Axv)	(y^4, y^8, y, y^5)	$y^{11}=1,$	$f=2^2,$	$k_0=\mathbb{F}_{2^{10}}$
(II, Axvi)	$(y^6, 1, y, y^3)$	$y^7=1,$	$f=1,$	$k_0=\mathbb{F}_{2^3}$
(II, Axvii)	(y^5, y^5, y, y^3)	$y^7=1,$	$f=2^2,$	$k_0=\mathbb{F}_{2^3}$
(II, Bi)	$(y^2, 1, y, y^2)$	$y^3=1,$	$f=1,$	$k_0=\mathbb{F}_{2^2}$
(II, Bii)	$(1, 1, y, y^{-1-2f})$	$y^{2f^2-1}=1$		
(II, Biii)	$(x, x^{1-2f}, 1, 1)$	$x^{2f^2-2f+1}=1$		
(II, Biv)	$(y^2, y^4, y, 1)$	$y^5=1,$	$f=2,$	$k_0=\mathbb{F}_{2^4}$

In particular, we see that the following solutions are simultaneously of type I and type II:

$$z=\left(y^{2+2f}, y^{2f}, y, y^{-1+2f}\right), \qquad y^{2f^2-1}=1,$$

which is type (II, Avii) and also type (I, Aix) after specializing $x=y^{1+2f}$;

$$z=\left(y^2, 1, y, y^2\right), \qquad y^3=1, \qquad f=1, \qquad k_0=\mathbb{F}_{2^2},$$

which is both types (I, Axii) and (II, Bi);

$$z=(x, x, 1, x), \qquad x^3=1, \qquad f=2, \qquad k_0=\mathbb{F}_{2^2},$$

which is both types (I, Axix) and (II, Axii).

2. Analysis of Eqs. (3m) and (4m)

The problem can be attacked as follows. Let f, z_i, $i=1,2,3,4$, be a solution. Equation (1) and either possibility in (2) provide us with two relations of type

$$z_1^A z_2^B z_3^C z_4^D = 1 \tag{5}$$

with A, B, C, D polynomials in f. Further relations of this type are obtained as follows.

The first step is to take advantage of the fact that Eqs. $(3m)$ and $(4m)$ are valid for every m. We start with the simpler equations $(3m)$.

Let us abbreviate

$$x_1 = z_1 z_2^{-1} z_3^{-1} z_4, \qquad x_2 = z_2 z_4^{-1}, \qquad x_3 = z_3 \tag{6}$$

and

$$y_1 = \left(z_1 z_2^{-1} z_3^{-1} z_4\right)^f, \qquad y_2 = \left(z_2 z_4^{-1}\right)^{2f}, \qquad y_3 = (z_3 z_4)^f. \tag{7}$$

We form the sixteen monomials

$$M_\mu = x_1^\alpha x_2^\beta x_3^\gamma \quad \text{with } \mu = \alpha + 2\beta + 4\gamma \quad \text{and}$$
$$M_\mu = y_1^\alpha y_2^\beta y_3^\gamma \quad \text{with } \mu = 8 + \alpha + 2\beta + 4\gamma,$$

$\alpha, \beta, \gamma = 0$ or 1. Thus Eq. $(3m)$ becomes

$$\sum_{\mu=0}^{15} M_\mu^m = 0.$$

Let $\xi_1, \ldots, \xi_s$ be the distinct values taken by the monomials M_μ, with multiplicities $\eta_1, \ldots, \eta_s$ taken mod 2. Then we have

$$\sum_{i=1}^{s} \xi_i^m \ \eta_i = 0$$

for $n = 0, 1, \ldots, s-1$. This is a linear system of Vandermonde type over the field k, with a solution $(\eta_1, \ldots, \eta_s)$. By construction, the ξ_i's are distinct and therefore the Vandermonde determinant does not vanish. This proves that $\eta_i = 0$ for each i. We have shown the following lemma.

Lemma 1. *The monomials M_μ, $\mu = 0, 1, \ldots, 15$, can be grouped in equal pairs. Conversely, if this is the case then $(3m)$ holds for every m.*

Since $M_0 = M_8$, and since (1) implies $M_7 = M_{15}$, we may remove these monomials from our consideration.

We proceed in the same way for Eq. $(4m)$. Let us abbreviate

$$u_1 = z_4, \qquad u_2 = z_4^2, \qquad u_3 = z_2 z_3^{-1},$$
$$u_4 = \left(z_3 z_4^{-1}\right)^2, \qquad u_5 = z_1 z_2^{-1} z_3^{-1} z_4^{-1} \tag{8}$$

and

$$v_1 = z_4^{4f}, \qquad v_2 = \left(z_2 z_3^{-1}\right)^{2f}, \qquad v_3 = \left(z_3 z_4^{-1}\right)^f,$$
$$v_4 = \left(z_3 z_4^{-1}\right)^{2f}, \qquad v_5 = \left(z_1 z_2^{-1} z_3^{-1} z_4^{-1}\right)^f. \tag{9}$$

We form the sixty-four monomials

$$N_\nu = u_1^\alpha u_2^\beta u_3^\gamma u_4^\delta u_5^\varepsilon \quad \text{with } \nu = \alpha + 2\beta + 4\gamma + 8\delta + 16\varepsilon \quad \text{and}$$
$$N_\nu = v_1^\alpha v_2^\beta v_3^\gamma v_4^\delta v_5^\varepsilon \quad \text{with } \nu = 32 + \alpha + 2\beta + 4\gamma + 8\delta + 16\varepsilon,$$

$\alpha, \beta, \gamma, \delta, \varepsilon = 0$ or 1. Equation $(4m)$ can be rewritten as

$$\sum_{\nu=0}^{63} N_\nu^m = 0.$$

Exactly as before, we obtain the next lemma.

Lemma 2. *The monomials N_ν, $\nu = 0, \dots, 63$, can be grouped in equal pairs. Conversely, if this is the case then $(4m)$ holds for every m.*

Since $N_0 = N_{32} = 1$, we may remove these monomials from our consideration.

3. Elimination of variables

We eliminate variables as follows. We start with Eq. (1). We set $x = z_1/z_3$ and $y = z_3$. Now Eqs. (1) and (2I) or (2II) determine z_2 and z_4 as functions of x and y. More precisely, we have

$$z_1 = xy, \qquad z_2 = (xy)^{1/f-1}, \qquad z_3 = y \tag{10}$$

and

$$z_4 = \begin{cases} x^{(1-2f^2)/f} y^{(1-f)/f} & \text{in Case I,} \\ x^{(1-2f+2f^2)/f} y^{(1-3f)/f} & \text{in Case II.} \end{cases} \tag{11}$$

The sixteen monomials $M_\mu = x^A y^B$ are given by their exponents $\{A, B\}$:

Case I: $\{0,0\}, \{2-2f,0\}, \{-1+2f,0\}, \{1,0\}, \{0,1\}, \{2-2f,1\}, \{-1+2f,1\}, \{1,1\}, \{0,0\}, \{2f-2f^2,0\}, \{-2f+4f^2,0\}, \{2f^2,0\}, \{1-2f^2,1\}, \{1+2f-4f^2,1\}, \{1-2f+2f^2,1\}, \{1,1\}$.

Case II: $\{0,0\}, \{2f,-2\}, \{1-2f,2\}, \{1,0\}, \{0,1\}, \{2f,-1\}, \{1-2f,3\}, \{1,1\}, \{0,0\}, \{2f^2,-2f\}, \{2f-4f^2,4f\}, \{2f-2f^2,2f\}, \{1-2f+2f^2,1-2f\}, \{1-2f+4f^2,1-4f\}, \{1-2f^2,1+2f\}, \{1,1\}$.

By Lemma 1, we have an equation $M_a = M_b$, where we may assume $b \neq 0, 7, 8, 15, a$. This gives us a relation

$$R = x^A y^B = 1 \tag{12}$$

for certain polynomials A, B in f.

Now consider the sixteen monomials M_μ. Let

$$M_\mu = x^C y^D.$$

We have, using (12):

$$M_\mu^A = R^{-C} M_\mu^A = y^{\Delta_\mu(f)}, \tag{13}$$

with

$$\Delta_\mu(f) = AD - BC. \tag{14}$$

In exactly the same way, we find

$$M_\mu^{-B} = x^{\Delta_\mu(f)} \quad \text{for all } \mu. \tag{15}$$

By Lemma 1, we may remove from the vector $\{\Delta_\mu(f)\}$ all components which appear an even number of times, and what is left must still be grouped in equal pairs. Now if $M_\mu = M_{\mu'}$ then (12) shows that

$$x^{D(f)} = 1, \qquad y^{D(f)} = 1 \tag{16}$$

with $D(f) = \Delta_\mu(f) - \Delta_{\mu'}(f)$.

We interpret (16) as giving an equation $D(f) = 0$ for the automorphism f, relative to its action on the elements $x = z_1/z_3$ and $y = z_3$ of k^*.

4. Solution of Eq. (3*m*), Case I

We begin by looking at the pairings $M_a = M_b$ and compute accordingly all possibilities for the exponent $\Delta_\mu(f)$. If the vector of exponents $\Delta_\mu(f)$ does not consists of equal pairs, we obtain a non-trivial list of possibilities for $D(f)$ as in (16).

The monomials M_μ, $\mu \neq 0, 7, 8, 15$, fall into two groups: $\mathcal{M}_1 = \{M_\mu\colon\ \mu = 1, 2, 3, 9, 10, 11\}$ and $\mathcal{M}_2 = \{M_\mu\colon\ \mu = 4, 5, 6, 12, 13, 14\}$. In the first group we have

$$\mathcal{M}_1 = \left\{x^\alpha\colon\ \alpha \in \left\{2-2f,\ -1+2f,\ 1,\ 2f-2f^2,\ -2f+4f^2,\ 2f^2\right\}\right\}, \tag{17}$$

while in the second group we have

$$\mathcal{M}_2 = \left\{y \cdot x^\beta\colon\ \beta \in \left\{0,\ 2-2f,\ -1+2f,\ 1-2f^2,\ 1+2f-4f^2,\ 1-2f+2f^2\right\}\right\}. \tag{18}$$

It is clear that Lemma 1 is satisfied if any one of

$$x^{f-1} = 1, \qquad x^{2f-1} = 1, \qquad x^{2f^2-1} = 1 \tag{19}$$

holds, because then for $i = 1, 2$ the monomials in $\mathcal{M}_i$ can be grouped in equal pairs.

It turns out that the elimination process described above conduces to a non-trivial equation for $D(f)$ precisely if we have a relation $M_a = M_b$ with $M_a \in \mathcal{M}_1$ and $M_b \in \mathcal{M}_2$. This gives us the following two essentially different situations.

Case AI. *For $i = 1, 2$ the monomials $M_\mu \in \mathcal{M}_i$ can be grouped in equal pairs.*

Case BI. *Case* AI *does not hold and there is at least one relation $M_a = M_b$ with $M_a \in \mathcal{M}_1$ and $M_b \in \mathcal{M}_2$.*

The following two lemmata settle the analysis of Eq. (3m), Case I.

Lemma 3. *Case* AI *holds if and only if one of*

$$x^{f-1} = 1, \qquad x^{2f-1} = 1, \qquad x^{2f^2-1} = 1 \tag{19}$$

holds.

Proof. In order to check that there are no other solution besides those given by (19), we start by looking at which monomial can be equal to M_3. We see that if (19) does not hold then either $M_3 = M_9$ and $x^{2f^2-2f+1} = 1$, or $M_3 = M_{10}$ and $x^{4f^2-2f-1} = 1$. If $M_3 = M_9$, we see that we must have $M_2 = M_{11}$, therefore $M_1 = M_{10}$ by exclusion. This gives $x^{4f^2-2} = 1$ and $x^{2f^2-1} = 1$, a case already covered by (19). If instead $M_3 = M_{10}$ then the monomials M_1, M_2, M_9, M_{11} must be equal in pairs and $x^{4f^2-2f-1} = 1$. If $M_1 = M_2$ then $x^{4f-3} = 1$, hence $x^4 = 1$ because the resultant of $4f^2 - 2f - 1$ and $4f - 3$ is -4, and finally $x = 1$. If $M_1 = M_9$ then $x^{2(f-1)^2} = 1$, and again $x = 1$ because the resultant of $4f^2 - 2f - 1$ and $(f-1)^2$ is 1. Thus we remain with $M_1 = M_{11}$, whence $M_2 = M_9$, yielding $x^{2f^2-1} = 1$, a case already covered by (19). This proves the lemma. □

Lemma 4. *A complete list of solutions of* (3m) *in Case* BI *is as follows*:

(i) $z = \left(y^{3-\frac{3}{2}f}, y^{\frac{3}{2}-\frac{3}{2}f}, y, y^{\frac{1}{2}-f}\right)$, $\quad y^{(f-1)^2} = 1$,
with $y^{f-1} \neq 1$;

(ii) $z = \left(y^3, y^{9-12f}, y, y^{11-16f}\right)$, $\quad y^{(2f-1)^2} = 1$,
with $y^{2f-1} \neq 1$;

(iii) $z = \left(x^{2f}, x^{2-2f}, x^{-1+2f}, x^{3-4f}\right)$, $\quad x^{(f-1)(2f-1)} = 1$,
with $x^{f-1} \neq 1$ *and* $x^{2f-1} \neq 1$;

(iv) $z = \left(1, 1, y, y^{-1+2f}\right)$, $\quad y^{2f^2-2f+1} = 1$;

(v) $z = \big(y^{11}, y^5, y, y^{17}\big)$, $y^{21} = 1$, $f = 2$, $k_0 = \mathbb{F}_{2^6}$;

(vi) $z = \big(x^{13}, x^{18}, x^{12}, x^8\big)$, $x^{21} = 1$, $f = 2^4$, $k_0 = \mathbb{F}_{2^6}$.

Proof. The Mathematica program "solveB.sastry", described and listed in Section 12, performs the elimination described before, obtaining a small list of possibilities for $D(f)$, namely:

$$3,\quad 5,\quad 7,\quad 9,\quad 21,\quad (f-1)^2,\quad (f-1)(2f-1),\quad (2f-1)^2,$$
$$3(2f^2-1),\quad 2f^2-2f+1.$$

In particular, we have $x^{D(f)} = y^{D(f)} = 1$.

We can immediately exclude $D(f) = 3,\ 5,\ 7,\ 9,\ 21$ as redundant. If, for example, $D(f) = 5$ then $x^5 = 1$, $k_0 = \mathbb{F}_{2^4}$, and $f = 1, 2, 4, 8$. Subcases $f = 1$ and $f = 8$ yield $x^{f-1} = 1$ and $x^{2f-1} = 1$, respectively, which however belong to Case AI. Subcases $f = 2$ and $f = 4$ imply $x^{2f^2-2f+1} = 1$, which is one of the possibilities allowed for $D(f)$. The other cases can be treated in the same way. Thus we remain with

$$D(f) = (f-1)^2,\ (f-1)(2f-1),\ (2f-1)^2,\ 3(2f^2-1),$$
$$2f^2-2f+1.$$

We start by listing the monomials M_i and reduce them using the relation $x^{D(f)} = 1$. This presents no problem for $D(f) = (f-1)^2$, $(f-1)(2f-1)$, $2f^2-2f+1$. If $D(f) = (2f-1)^2$, we work with the monomials M_i^2; this is possible because we are in characteristic 2. If instead $D(f) = 3(2f^2-1)$, we have to be more careful, because cubing the monomials M_i leads to no information. Thus in this last case we reduce the monomials using the relation $x^{2f^2-1} = \varepsilon$, where $\varepsilon^3 = 1$ and $\varepsilon \neq 1$. Note that we cannot have $x^3 = 1$, because then either $x^{f-1} = 1$ or $x^{2f-1} = 1$, which belong to Case AI.

After performing this reduction we still have to check Lemma 1. The calculation turns out to be sufficiently small to be done by hand. In any case, the Mathematica program "refineB.sastry" quickly produces the following possibilities, not necessarily covered by (19):

$$x^{(f-1)^2} = 1, \qquad x^{4-6f}y = 1;$$
$$x^{(f-1)(2f-1)} = 1, \qquad x^{-1}y = 1, \qquad x^{3(f-1)} = 1;$$
$$x^{(f-1)(2f-1)} = 1, \qquad x^{1-2f}y = 1;$$
$$x^{(f-1)(2f-1)} = 1, \qquad x^{1-3f}y = 1, \qquad x^{3(2f-1)} = 1;$$
$$x^{(2f-1)^2} = 1, \qquad x^{-1}y^2 = 1;$$
$$x^{2f^2-2f+1} = 1, \qquad xy = 1;$$
$$x^{2f^2-1} = \varepsilon, \qquad x^{-2+2f}y = 1, \qquad x^{21} = 1.$$

The two cases $x^{(f-1)(2f-1)} = 1$, $x^{-1}y = 1$, $x^{3(f-1)} = 1$ and $x^{(f-1)(2f-1)} = 1$, $x^{1-3f}y = 1$, $x^{3(2f-1)} = 1$ are eliminated by substituting $y = x$ and $y = x^{3f-1}$ in the set of reduced monomials and checking directly that Lemma 1 forces (19) to hold. The remaining cases yield the solutions listed in Lemma 4, completing the proof. □

5. Solution of Eq. (3*m*), Case II

We proceed in a similar fashion as in the analysis of Case II. Then we find that the elimination process described before conduces to a trivial equation for $D(f)$ whenever there is an equality between monomials corresponding to an edge of the graph G on Fig. 1 where vertices are monomials M_i and edges between vertices i and j correspond to an equation $M_i = M_j$.

As before, this leads to two cases as follows.

Case AII. *The graph of relations among the monomials M_i has at least one edge in common with G.*

Case BII. *All relations $M_a = M_b$ are outside G.*

The following two lemmata settle the analysis of Eq. (3*m*), Case II.

Lemma 5. *Case* AII *holds if and only if one of*

$$x^{2f-1}y^{-2} = 1, \qquad x^f y^{-1} = 1, \qquad x^{-2f^2}y^{2f+1} = 1 \tag{20}$$

holds.

Proof. Immediate, by direct computation of the relations corresponding to the edges of G. □

Lemma 6. *A complete list of solutions of* (3*m*) *in Case* BII *is as follows*:

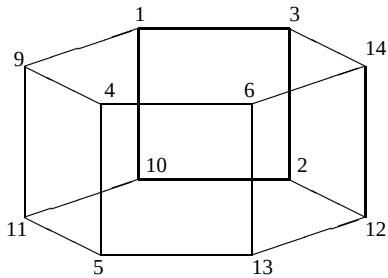

Fig. 1. The graph G.

(i) $z = \left(x^{2f}, x^{2-2f}, x^{-1+2f}, x^{3-4f}\right)$, $x^{(f-1)(2f-1)} = 1$,
with $x^{f-1} \neq 1$ *and* $x^{2f-1} \neq 1$;

(ii) $z = \left(1, 1, y, y^{-1-2f}\right)$, $y^{2f^2-1} = 1$;

(iii) $z = \left(x, x^{1-2f}, 1, 1\right)$, $x^{2f^2-2f+1} = 1$;

(iv) $z = \left(y^{3-3f}, y^{-3f}, y, y^{-1-2f}\right)$, $y^{2f^2-2f+1} = 1$;

(v) $z = \left(y^3, y^{6-6f}, y, y^{2-2f}\right)$, $y^{(f-1)(2f-1)} = 1$,
with $y^{f-1} \neq 1$ *and* $y^{2f-1} \neq 1$;

(vi) $z = \left(y^8, y^5, y, y^6\right)$, $y^9 = 1$, $y^3 \neq 1$, $f = 2$, $k_0 = \mathbb{F}_{2^6}$.

Proof. The Mathematica program "solveB.sastry" produces a reasonably small list of possibilities for $D(f)$, namely:

$$3,\quad 5,\quad 9,\quad 15,\quad 2f-1,\quad (f-1)(2f-1),\quad 2f^2-1,\quad f-1,$$
$$2f+1,\quad 2f^2+2f-1,\quad 2f^2-2f+1,$$

by looking at a relation $M_2 = M_i$, and

$$3,\quad 5,\quad 9,\quad 15,\quad 2f-1,\quad (f-1)(2f-1),\quad 2f^2-1,\quad f-1,$$
$$f+1,\quad 2f^2-2f-1,\quad 2f^2-2f+1,$$

by looking at a relation $M_9 = M_i$. Any possible $D(f)$ must be compatible with both lists. Now we can eliminate the possibilities $f+1$ and $2f+1$ as redundant, by looking at the resultant with the possibilities of $D(f)$ in the other list. Similarly, the possibilities $D(f) = f-1$, $2f-1$ are a consequence of $D(f) = (f-1)(2f-1)$. Thus we remain with

$$D(f) = 3,\ 5,\ 9,\ 15,\ (f-1)(2f-1),\ 2f^2-1,\ 2f^2-2f+1.$$

As in the proof of Lemma 4, we start by listing the monomials M_i and reduce them using the relation $x^{D(f)} = 1$, and after performing this reduction we still have to satisfy Lemma 1. The Mathematica program "refineB.sastry" quickly produces, besides $D(f) = 3, 5, 9, 15$, the following possibilities, not necessarily covered by (20):

$$D(f) = f-1, \qquad x^{-1}y = 1;$$
$$D(f) = f-1, \qquad x^{-2+4f}y^{1-4f} = 1;$$
$$D(f) = 2f-1, \qquad x^{-2+4f}y^{1-4f} = 1;$$
$$D(f) = 3(2f-1), \qquad x^{(f-1)(2f-1)} = y^{(f-1)(2f-1)} = 1,$$
$$x^{-2+4f}y^{1-4f} = 1;$$
$$D(f) = f-1, \qquad x^{-2+3f}y^{-2f} = 1;$$

$$D(f) = (f-1)(2f-1), \qquad x^{-1+2f}y^{-1} = 1;$$
$$D(f) = (f-1)(2f-1), \qquad x^{-f}y^{2f} = 1;$$
$$D(f) = f-1, \qquad x^{-2f}y^{3} = 1;$$
$$D(f) = 2f-1, \qquad x^{1-4f}y^{4f} = 1;$$
$$D(f) = 7, \qquad x^{2f^2-1} = y^{2f^2-1} = 1, \qquad x^{-3+2f}y^{4f} = 1;$$
$$D(f) = 7, \qquad x^{2f^2-1} = y^{2f^2-1} = 1, \qquad x^{-2f}y^{3} = 1;$$
$$D(f) = 2f^2-1, \qquad x^{1-2f}y^{1-2f} = 1;$$
$$D(f) = 13, \qquad x^{2f^2-2f-1} = y^{2f^2-2f-1} = 1, \qquad x^{-3}y^{-1+4f} = 1;$$
$$D(f) = 13, \qquad x^{2f^2-2f-1} = y^{2f^2-2f-1} = 1, \qquad x^{-4-2f}y^{-1+6f} = 1;$$
$$D(f) = 2f^2-2f+1, \qquad y^{2f} = 1;$$
$$D(f) = 2f^2-2f+1, \qquad x^{-2+2f}y^{1-4f} = 1.$$

These possibilities are not independent of (20). In fact, we check that the cases with $D(f) = f-1$ and $D(f) = 2f-1$ are specializations of (20). Also $D(f) = 7$ is a specialization of $D(f) = 2f^2-1$. The cases $D(f) = 13$ imply $f = 2^8$ or 2^9. The first choice $f = 2^8$ implies that the corresponding relations $x^{-3}y^{-1+4f} = 1$ and $x^{-4-2f}y^{-1+6f} = 1$ are special cases of (20), while for the second choice $f = 2^9$ we see directly that Lemma 1 is not satisfied.

The case $D(f) = 3(2f-1)$,

$$x^{(f-1)(2f-1)} = y^{(f-1)(2f-1)} = 1, \qquad x^{-2+4f}y^{1-4f} = 1$$

is treated as follows. From $x^{-2+4f}y^{1-4f} = 1$ we obtain $y^{(1-4f)(1-f)} = 1$, and using $y^{(f-1)(2f-1)} = 1$ we find $y^{f-1} = 1$. This last equation and $y^{3(2f-1)} = 1$ show that $y^3 = y^{f-1} = 1$, whence $y^{1-4f} = 1$. Now the relation $x^{-2+4f}y^{1-4f} = 1$ becomes $x^{-2+4f} = 1$ and $x^{2f-1} = 1$. Thus we must have $x^{2f-1} = 1$, $y^3 = y^{f-1} = 1$. Now we reduce the monomials M_i accordingly and check that Lemma 1 is satisfied only if one of $x = 1$, $y = 1$, $xy = 1$, $xy^2 = 1$ holds. The first three possibilities are covered by (20), while the last possibility implies $x^3 = 1$, hence $D(f) = 3$.

In the remaining five cases we express x in terms of y whenever possible, and y in terms of x otherwise. We check, using the Mathematica program "verify.sastry", that the monomials M_i satisfy Lemma 1, obtaining in the end the list of solutions (i)–(v) in Lemma 6.

It remains to verify that the cases $D(f) = 3, 5, 9, 15$ are covered by the list we have obtained or by (20), and this is done easily by checking directly the various possibilities for f, obtaining the further solution (vi) for $D(f) = 9$.

6. Solution of Eq. (4m), Cases BI and BII

In this section we bring in the information obtained by the solution of Eq. (3m) into Eq. (4m). We begin with Cases BI and BII, for which the final analysis is quite simple.

We substitute the parameterizations given by Lemmata 4 and 6 into Eq. (4m), for example, using the Mathematica program "verify.sastry". Then we determine the cases in which Lemma 2 holds, for example by applying the function RedDeg[ ] described in Section 12 to the vector of monomials N_j. Thus we see that the types listed in Lemmata 4 and 6 reduce to:

Case I, type (i): $D(f) = 3, 9$;
Case I, type (ii): $D(f) = 3, 7, 9, 21$;
Case I, type (iii): $D(f) = 3$;
Case I, type (iv): no solutions;
Case I, type (v): $D(f) = 3, 7$;
Case I, type (vi): $D(f) = 3, 7$;
Case II, type (i): $D(f) = 3$;
Case II, type (ii): $D(f) = 2f^2 - 1$;
Case II, type (iii): $D(f) = 2f^2 - 2f + 1$;
Case II, type (iv): $D(f) = 5$;
Case II, type (v): $D(f) = 3, 5, 7, f - 1, 2f - 1$;
Case II, type (vi): $D(f) = 3$.

We must exclude from this list Cases AI and AII. The final result is as follows:

- Case I, types (i) and (ii) with $D(f) = 9$ yield two solutions, listed in Table 1 as (I, Bi) and (I, Bii).
- Case II, type (i) and $D(f) = 3$ yields the solution listed in Table 2 as (II, Bi).
- Case II, types (ii) and (iii) are solutions, listed in Table 2 as (II, Bii), (II, Biii).
- Case II, type (iv), $D(f) = 5$ gives two solutions, one listed in Table 2 as (II, Biv) and the other a specialization of (II, Biii).

This completes the analysis of Sastry automorphisms in Cases BI and BII.

7. Solution of Eq. (4m), Case AI. First reductions

The analysis of this case leads to many subcases. We recall that Case AI is characterized by a relation $x^m = 1$ with m one of $f - 1, 2f - 1, 2f^2 - 1$.

We set $Y = y^m$ and apply Lemma 2 to the monomials N_j^m first. The advantage in doing this is that in this way we have to deal with equations with monomials in the single variable Y rather than two variables x, y.

After doing this we remove equal pairs of monomials and remain with a set of 28 monomials, which by Lemma 2 must again be equal in pairs. The exponents of these monomials are[2] as follows:

$$\{-1,\ 1,\ 4-5f,\ 3-4f,\ 3-3f,\ 2-2f,\ 2-f,\ -1+f,\ -2f^2,\ 2f^2,$$
$$1+f,\ -2+2f,\ -2+3f,\ -3+4f,\ -3+5f,\ -4+6f,\ 6f-8f^2,$$
$$4f-6f^2,\ 5f-6f^2,\ 2f-4f^2,\ 3f-4f^2,\ f-2f^2,\ f+2f^2,$$
$$-2f+4f^2,\ -f+4f^2,\ -4f+6f^2,\ -3f+6f^2,\ -5f+8f^2\}.$$

This yields a non-trivial relation of the type $Y^{d(f)}=1$. Let U_i, $i=1,\dots,28$, be the 28 monomials which must satisfy Lemma 2. The Mathematica program "presolveAI.sastry", described below, produces a list of possibilities for $d(f)$ in the following manner.

Firstly, by considering a relation $U_2=U_i$, we find that $d(f)$ is one of

$$5,\quad 9,\ f-1,\quad 3(f-1),\quad 2f-1,\quad 3(2f-1),\quad 2f^2-1.$$

Then, by considering a relation $U_7=U_i$, we find that $d(f)$ is also one of

$$5,\quad 9,\quad f-1,\quad 5(f-1),\quad 2f-1,\quad 2f^2-1.$$

It follows easily from this that we may take

$$d(f)=5,\ 9,\ f-1,\ 2f-1,\ 2f^2-1.$$

The Mathematica program "solveAI.sastry" now can be used to analyze more closely Eq. (4m).

If $x^{f-1}=1$ and $y^{(f-1)^2}=1$, we reduce the monomials N_j modulo the relations $x^{f-1}=1$ and $y^{(f-1)^2}=1$ and remove equal pairs of monomials, remaining with 40 monomials U_i, $i=1,\dots,40$. If we consider a relation $U_{11}=U_i$, we see that $D(f)$ can be as follows:

$$D(f)=3,5,7,9,15,21,25,49;$$
$$D(f)=\{1,3,5,7,9,15\}\cdot(f-1);$$
$$D(f)=(f-1)^2\quad\text{if } x^{-1}y^{1-f}=1.$$

If $x^{-1}y^{1-f}=1$, we have a solution, listed in Table 1 as (I, Ai).

If $x^{f-1}=1$ and $y^{(f-1)(2f-1)}=1$, we reduce the monomials N_j modulo the relations $x^{f-1}=1$ and $y^{(f-1)(2f-1)}=1$ and remove equal pairs of monomials, remaining with 44 monomials U_i, $i=1,\dots,44$. If we consider a relation $U_4=U_i$, we see that $D(f)$ can be as follows:

[2] Here and in what follows we order these monomials according to the lexicographic order provided by Mathematica.

$$D(f) = 3, 5, 7, 9, 11, 13, 15, 17, 21, 27, 35, 45, 63, 75, 105;$$
$$D(f) = \{1, 3, 5, 7, 9, 15\} \cdot (f-1);$$
$$D(f) = \{1, 5\} \cdot (2f-1);$$
$$D(f) = (f-1)(2f-1) \quad \text{if } x^{-1}y^{1-2f} = 1 \text{ or } y^{1-2f} = 1.$$

If $x^{-1}y^{1-2f} = 1$, we have a solution, listed in Table 1 as (I, Aii). If instead $y^{2f-1} = 1$, we have the solution listed in Table 1 as (I, Aiii).

If $x^{f-1} = 1$ and $y^{(f-1)(2f^2-1)} = 1$, we reduce the monomials N_j modulo the relations $x^{f-1} = 1$ and $y^{(f-1)(2f^2-1)} = 1$ and remove equal pairs of monomials, remaining with 48 monomials U_i, $i = 1, \ldots, 48$. If we consider a relation $U_1 = U_i$, we see that $D(f)$ can be:

$$D(f) = 3, 5, 7, 9, 15, 21, 25, 49, 63;$$
$$D(f) = \{1, 5, 9\} \cdot (f-1);$$
$$D(f) = 2f^2 - 1 \quad \text{if } x = 1.$$

The case $x = 1$ is a specialization of (I, Aix) in Table 1.

If $x^{2f-1} = 1$ and $y^{(f-1)(2f-1)} = 1$, we reduce the monomials N_j modulo the relations $x^{2f-1} = 1$ and $y^{(f-1)(2f-1)} = 1$ and remove equal pairs of monomials, remaining with 44 monomials U_i, $i = 1, \ldots, 44$. If we consider a relation $U_5 = U_i$, we see that $D(f)$ can be:

$$D(f) = 3, 5, 7, 9, 11, 15, 21, 25, 27, 33, 35;$$
$$D(f) = f - 1;$$
$$D(f) = \{1, 3, 5, 9\} \cdot (2f-1);$$
$$D(f) = (f-1)(2f-1) \quad \text{if } x^{-1}y^{-4+4f} = 1 \text{ or } x^{-1}y^{-2+2f} = 1.$$

If $x^{-1}y^{-4+4f} = 1$ or $x^{-1}y^{-2+2f} = 1$, we have solutions listed in Table 1 as (I, Aiv) and (I, Av).

If $x^{2f-1} = 1$ and $y^{(2f-1)^2} = 1$, we reduce the monomials N_j modulo the relations $x^{2f-1} = 1$ and $y^{(2f-1)^2} = 1$ and remove equal pairs of monomials, remaining with 40 monomials U_i, $i = 1, \ldots, 40$. If we consider a relation $U_3 = U_i$, we see that $D(f)$ can be:

$$D(f) = 3, 5, 7, 9, 15, 21, 25, 27, 49, 81;$$
$$D(f) = \{1, 3, 5, 7, 9, 15\} \cdot (2f-1);$$
$$D(f) = (2f-1)^2 \quad \text{if } x^{-1}y^{-2+4f} = 1.$$

If $x^{-1}y^{-2+4f} = 1$, we have a solution listed in Table 1 as (I, Avi).

If $x^{2f-1} = 1$ and $y^{(2f-1)(2f^2-1)} = 1$, we reduce the monomials N_j modulo the relations $x^{2f-1} = 1$ and $y^{(2f-1)(2f^2-1)} = 1$ and remove equal pairs of

monomials, remaining with 48 monomials U_i, $i = 1, \dots, 48$. If we consider a relation $U_1 = U_i$, we see that $D(f)$ can be:

$$D(f) = 3, 5, 7, 9, 15, 21, 35, 63;$$
$$D(f) = \{1, 5, 9\} \cdot (2f - 1);$$
$$D(f) = 2f^2 - 1 \quad \text{if } x^3 = 1.$$

In this last case, since we are assuming $x^{2f-1} = 1$ we deduce $x = 1$, $D(f) = 2f^2 - 1$, a case examined before.

The situation in case $x^{2f^2-1} = 1$ is rather different. In this case we see that $y^{f-1} = 1$, $y^{2f-1} = 1$, $y^{2f^2-1} = 1$ are solutions to $(4m)$. This gives the solutions numbered (I, Avii), (I, Aviii), (I, Aix) in Table 1.

We know already that we can take $D(f) = 5(2f^2 - 1)$, $9(2f^2 - 1)$ or $d(f)(2f^2 - 1)$ with $d(f) = f - 1, 2f - 1, 2f^2 - 1$, and we now proceed to refine this list. The Mathematica program "solveAIiii.sastry", described below, produces either a new value for $D(f)$ or an exponent $E(f)$ for which $y^{E(f)} = 1$.

This program works as follows. We reduce the monomials N_i modulo the relation $x^{2f^2-1} = 1$ and remove equal pairs, obtaining a list of 52 new monomials, which again must be equal in pairs. We equate a monomial $x^f y^a$ to other monomials in every possible way, obtaining a relation of type $x^a y^b = 1$ with $a = 0$, f, $-1 + 2f$, $1 - f$. If $a \neq 0$, this is equivalent to a relation $xy^u = 1$ for a certain $u = u(f)$, and we can eliminate x. If instead $a = 0$ then we have $y^b = 1$, which we combine with our preceding information on $D(f)$.

We exclude at the present moment the possibilities $D(f) = 3(2f^2 - 1)$, $5(2f^2 - 1)$, $9(2f^2 - 1)$, which will be examined later on.

If $D(f) = (f - 1)(2f^2 - 1)$ then $x^{-1+2f} y^{-2+2f} = 1$ (equivalently, $x^{1-f} y^{-2f+2f^2} = 1$ and $x^f y^{-2+2f^2} = 1$) leads to the solution numbered (I, Ax). The remaining possibilities are as follows.

If we equate the monomial $x^f y^{-2+3f}$ to another monomial we find, besides $D(f) = 1$, 3, $f - 1$, $2f - 1$, $2f^2 - 1$ and $E(f) = f - 1$, $2f - 1$, $2f^2 - 1$, which all lead to solutions which have been examined already, that we must have: $D(f) = 5$, 7, 23, 31, $3(2f^2 - 1)$, $E(f) = 7$, 21 and a further possibility $D(f) = 7(f - 1)$.

If instead we equate the monomial $x^f y^{4f-6f^2}$ to another monomial we find, besides the known solutions, we can only have $D(f) = 5$, 7, $3(-1 + 2f^2)$, $5(2f^2 - 1)$, $9(2f^2 - 1)$, $15(2f^2 - 1)$.

Now $D(f)$ must be either a known case or a possibility in both lists we have obtained. Since $f - 1$ and $2f^2 - 1$ are always coprime, we can eliminate $D(f) = 7(f - 1)$ and $D(f) = 15(2f^2 - 1)$ as leading to $D(f) = 105$ or to $D(f) = 2f^2 - 1$.

Thus we remain with $D(f) = 5$, 7, 23, 31, 105, $3(-1 + 2f^2)$, $5(2f^2 - 1)$, $9(2f^2 - 1)$, $E(f) = 7, 21$.

If $D(f) = (2f-1)(2f^2-1)$ then $x^{1-f}y^{1-2f} = 1$ (equivalently, $x^f y^{1-4f^2} = 1$ and $x^{-1+2f}y^{2f-4f^2} = 1$) leads to the solution numbered (I, Axi).

If we equate the monomial $x^f y^{-3+4f}$ to another monomial we find, besides the known solutions, we can only have

$$D(f) = 7,\ 3\big(2f^2-1\big),\ 5\big(2f^2-1\big),\ 9\big(2f^2-1\big),\ 15\big(2f^2-1\big).$$

Finally if $D(f) = (2f^2-1)^2$ then equating the monomial $x^f y^{-1+2f}$ to another monomial shows that

$$D(f) = 7,\ 23,\ 3\big(2f^2-1\big),\ 5\big(2f^2-1\big),\ 7\big(2f^2-1\big),\ 9\big(2f^2-1\big).$$

8. Completion of solution of Eq. (4*m*), Case AI, $x^{f-1} = 1$

In this case we still have to consider the following possibilities: $D(f) \in \mathcal{D}$, with

$$\mathcal{D} = \{3, 5, 7, 9, 11, 13, 15, 17, 21, 25, 27, 35, 45, 49, 63, 75, 105\}; \tag{21}$$
$$D(f) = \{1, 3, 5, 7, 9, 15\} \cdot (f-1);$$
$$D(f) = \{1, 5\} \cdot (2f-1).$$

Let us consider the possibility $D(f) = c \cdot (f-1)$ with c one of $1, 3, 5, 7, 9, 15$. We apply the program "refineAI.sastry" using $D(f) = c \cdot (f-1)$. Using a relation $U_4 = U_i$, we see that either

$$D(f) \in \{1, 3, 5, 7, 9\} \cdot \mathcal{D} \tag{22}$$

or we have a relation $x^a y^b = 1$ with $\{a, b\}$ one of

$$\{7, 0\} \cdot c, \quad \{3, 0\} \cdot c, \quad \{1, 0\} \cdot c, \quad \{1, 1\} \cdot c, \quad \{0, 1\} \cdot c.$$

A second run of the same program but using a relation $U_6 = U_i$ yields that either

$$D(f) \in \{1, 3, 5, 7, 9\} \cdot \mathcal{D} \tag{22}$$

or we have a relation $x^a y^b = 1$ with $\{a, b\}$ one of

$$\{5, 0\} \cdot c, \quad \{1, 0\} \cdot c, \quad \{1, 1\} \cdot c, \quad \{0, 3\} \cdot c.$$

Thus we see that either (22) holds or we have that a relation $x^a y^b = 1$ holds with $\{a, b\}$ one of

$$\{1, 0\} \cdot c, \quad \{1, 1\} \cdot c.$$

We analyze these possibilities with the Mathematica program "solveAIi.sastry". We obtain either $D(f) \in \{1, 3, 5, 7, 9, 15, 21, 27, 45\}$ or known cases. More precisely, the cases $\{a, b\} = \{1, 0\} \cdot c$ are a specialization of (I, Ai) and the cases $\{a, b\} = \{1, 1\} \cdot c$ are a specialization of (I, Aii).

If $D(f) = 2f - 1$ then we have $x^{f-1} = 1$ and $y^{2f-1} = 1$, which is a special case of (I, Aiii). Thus it remains the case $D(f) = 5(2f - 1)$. This and $x^{f-1} = 1$ imply $x^5 = 1$. Now the program "solveAIi.sastry" shows that either $D(f) \in \{1, 3, 5, 7, 9, 15, 21, 27, 45\}$ or we obtain the known case (I, Aii).

It remains to test the cases

$$D(f) = \begin{array}{l} 3, 5, 7, 9, 11, 13, 15, 17, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 63, 65, \\ 75, 77, 81, 85, 91, 99, 105, 117, 119, 125, 135, 147, 153, 165, 175, 189, \\ 195, 225, 243, 245, 255, 315, 343, 375, 405, 441, 525, 567, 675, 735, \\ 945, 1125, 1575. \end{array}$$

Here, in order to reduce the size of the calculation, it is convenient to keep in mind that $D(f)$ divides $d(f)(f - 1)$, with $d(f)$ one of $5, 9, f - 1, 2f - 1, 2f^2 - 1$. The program "refineAIi.sastry" now produces the following seven new solutions:

$$\begin{array}{lllll} D(f) = 3, & f = 1, & x = y, & y^3 = 1, & k_0 = \mathbb{F}_{2^2}; \\ D(f) = 5, & f = 2, & x = 1, & y^5 = 1, & k_0 = \mathbb{F}_{2^2}; \\ D(f) = 5, & f = 2^2, & x = 1, & y^5 = 1, & k_0 = \mathbb{F}_{2^2}; \\ D(f) = 7, & f = 1, & x = y^4, & y^7 = 1, & k_0 = \mathbb{F}_{2^3}; \\ D(f) = 7, & f = 1, & x = y^2, & y^7 = 1, & k_0 = \mathbb{F}_{2^3}; \\ D(f) = 9, & f = 2, & x = 1, & y^9 = 1, & k_0 = \mathbb{F}_{2^6}; \\ D(f) = 9, & f = 2^4, & x = 1, & y^9 = 1, & k_0 = \mathbb{F}_{2^6}; \end{array}$$

listed as (I, Axii)–(I, Axviii). Note that (I, Axii) coincides with (II, Bi).

9. Completion of solution of Eq. (4*m*), Case AI, $x^{2f-1} = 1$

We proceed as in the preceding section. In this case we still have to consider the following possibilities: $D(f) \in \mathcal{D}$, with

$$\begin{aligned} &\mathcal{D} = \{3, 5, 7, 9, 11, 15, 21, 25, 27, 33, 35, 49, 63, 81\}; \qquad (23) \\ &D(f) = \{1, 3, 5, 7, 9, 15\} \cdot (2f - 1); \\ &D(f) = f - 1. \end{aligned}$$

Let us consider the possibility $D(f) = c \cdot (2f - 1)$ with c one of 1, 3, 5, 7, 9, 15. We apply the program "refineAI.sastry" using $D(f) = c \cdot (2f - 1)$. Using a relation $U_2 = U_i$, we see that either

$$D(f) \in \{1, 3, 5, 7, 9\} \cdot \mathcal{D} \qquad (24)$$

or we have a relation $x^a y^b = 1$ with $\{a, b\}$ one of

$$\{5, 5\} \cdot c, \quad \{1, 2\} \cdot c, \quad \{1, 1\} \cdot c, \quad \{1, 0\} \cdot c.$$

A second run of the same program using a relation $U_4 = U_i$ yields that either

$$D(f) \in \{1, 3, 5, 7\} \cdot \mathcal{D} \tag{25}$$

or we have a relation $x^a y^b = 1$ with $\{a, b\}$ one of

$$\{5, 0\} \cdot c, \quad \{3, 6\} \cdot c, \quad \{1, 2\} \cdot c, \quad \{1, 1\} \cdot c, \quad \{1, 0\} \cdot c, \quad \{0, 1\} \cdot c.$$

Thus we see that either (24) holds or we have that a relation $x^a y^b = 1$ holds with $\{a, b\}$ one of

$$\{1, 0\} \cdot c, \quad \{1, 1\} \cdot c, \quad \{1, 2\} \cdot c.$$

We analyze these possibilities with the Mathematica program "solveAIii.sastry", obtaining correspondingly known cases (I, Avi), (I, Av), (I, Aiv) or $D(f)$ in the list (25).

If instead $D(f) = f - 1$, the hypothesis $x^{2f-1} = 1$ implies $x = 1$, a situation covered by the analysis of the preceding section. Thus it remains to test the cases

$$\begin{aligned} D(f) = {} & 3, 5, 7, 9, 11, 15, 21, 25, 27, 33, 35, 45, 49, 55, 63, 75, 77, 81, 99, 105, \\ & 125, 135, 147, 165, 175, 189, 225, 231, 243, 245, 297, 315, 343, 375, \\ & 405, 441, 495, 567, 729, 735, 945, 1215. \end{aligned}$$

Here again, in order to reduce the size of the calculation, it is convenient to keep in mind that $D(f)$ divides $d(f)(2f - 1)$, with $d(f)$ one of $5, 9, f - 1, 2f - 1$, $2f^2 - 1$. The program "refineAIii.sastry" now produces the following three new solutions:

$$\begin{aligned} &D(f) = 3, \quad f = 2, \quad x^3 = 1, \quad y = 1, \quad k_0 = \mathbb{F}_{2^2}; \\ &D(f) = 7, \quad f = 2^2, \quad x^7 = 1, \quad y = x^4, \quad k_0 = \mathbb{F}_{2^3}; \\ &D(f) = 7, \quad f = 2^2, \quad x^7 = 1, \quad y = x^5, \quad k_0 = \mathbb{F}_{2^3} \end{aligned}$$

listed as (I, Axix)–(I, Axxi). Note that the solution (I, Axix) coincides with the solution (II, Axii).

10. Completion of solution of Eq. (4*m*), Case AI, $x^{2f^2-1} = 1$

It remains to analyze the cases $D(f) = 5$, 7, 23, 31, 105, $3(-1 + 2f^2)$, $5(2f^2 - 1)$, $7(2f^2 - 1)$, $9(2f^2 - 1)$, $15(2f^2 - 1)$ and the possibility $x^{2f^2-1} = 1$, $y^c = 1$ with $c = 7, 21$. We may remove the case $D(f) = 5$, since it leads to $x = 1$.

If $y^{c\cdot(2f^2-1)} = 1$ with $c = 3, 5, 7, 9, 15$ then the program "refineAIiii.sastry" shows that either we are in the known case (I, Axi), or $x^{2f^2-1} = 1$ and $y^{n\cdot c} = 1$ with $n = 1, 7, 9$, or $D(f) = n \cdot c$ with n in the following list:

$$\begin{aligned} &1, 7, 9, 17, 23, 25, 31, 41, 47, 49, 63, 71, 73, 79, 81, 89, 97, 103, \\ &113, 119, 161, 167. \end{aligned}$$

The same program deals with the cases $x^{2f^2-1}=1$, $y^c=1$ with

$$c=3,\ 5,\ 7,\ 9,\ 15,\ 21,\ 27,\ 35,\ 45,\ 49,\ 63,\ 81,\ 105,\ 135.$$

Then we see that either we have cases (I, Avii), (I, Aviii), (I, Aix) or $x^c=1$. We may suppose $x\neq 1$, which eliminates the cases $c=3,5,9,27,45,81,135$, yielding $D(f)=7,21,35,49,63,105$. In conclusion, it remains to test the finite list

$$\begin{aligned} D(f) = {} & 3,\ 5,\ 7,\ 9,\ 15,\ 17,\ 21,\ 23,\ 25,\ 27,\ 31,\ 35,\ 41,\ 45,\ 47,\ 49\ ,\ 51,\ 63,\ 69,\ 71,\\ & 73,\ 75,\ 79,\ 81,\ 85,\ 89,\ 93,\ 97,\ 103,\ 105,\ 113,\ 115,\ 119,\ 123,\ 125,\ 135,\\ & 141,\ 147,\ 153,\ 155,\ 161,\ 167,\ 175,\ 189,\ 205,\ 207,\ 213,\ 217,\ 219,\ 225,\\ & 235,\ 237,\ 243,\ 245,\ 255,\ 267,\ 279,\ 287,\ 291,\ 309,\ 315,\ 329,\ 339,\ 343,\\ & 345,\ 355,\ 357,\ 365,\ 369,\ 375,\ 395,\ 405,\ 423,\ 441,\ 445,\ 465,\ 483,\ 485,\\ & 497,\ 501,\ 511,\ 515,\ 553,\ 565,\ 567,\ 595,\ 615,\ 623,\ 639,\ 657,\ 679,\ 705,\\ & 711,\ 721,\ 729,\ 735,\ 791,\ 801,\ 805,\ 833,\ 835,\ 873,\ 927,\ 945,\ 1017,\ 1065,\\ & 1071,\ 1095,\ 1127,\ 1169,\ 1185,\ 1215,\ 1335,\ 1449,\ 145\ 5,\ 1503,\ 1545,\\ & 1695,\ 1785,\ 2415,\ 2505. \end{aligned}$$

The last part of the program "refineAIiii.sastry" checks that no new cases arise from this list, completing the analysis.

11. Solution of Eq. (4*m*), Case AII

We must consider the three relations $x^{-1+2f}y^{-2}=1$, $x^fy^{-1}=1$, $x^{-2f^2}y^{1+2f}=1$. The elimination procedure described in Section 3 applied to the monomials N_i produces, after removing the pairs of equal elements, a new vector U_k of monomials. We perform the last elimination using the Mathematica program "solveAII.sastry" described in Section 12.

Relation $x^{-1+2f}y^{-2}=1$.
If we use the relation $U_2=U_k$ we obtain the following possibilities:

$$\begin{aligned} D(f) &= 3,5,7,9,11,15,23,25,27,45;\\ D(f) &= f-1,\ 3(f-1),\ 7(f-1),\ 2f+1,\ 5(2f+1),\\ &\quad (f-1)(2f+1),\ 3(f-1)(2f+1),\ 2f^2-1,\ 4f^2-2f-1. \end{aligned}$$

If we use the relation $U_3=U_k$ we obtain the following possibilities:

$$\begin{aligned} D(f) &= 3,5,7,9,11;\\ D(f) &= 3(f-1),\ (f-1)(2f+1),\ 2f^2-1,\ 4f^2-2f-1,\\ &\quad 3\big(4f^2-2f-1\big). \end{aligned}$$

If we use the relation $U_6=U_k$ we obtain the following possibilities:

$$D(f) = 3, 5, 7, 9, 11, 15, 21, 23, 25, 27;$$
$$D(f) = f-1,\ 2f+1,\ 3(2f+1),\ 5(2f+1),\ (f-1)(2f+1),$$
$$2f^2-1,\ 4f^2-2f-1,\ 3\big(4f^2-2f-1\big).$$

Any $D(f)$ must divide some possibility in each of these three groups. Since the resultant of $(f-1)(2f+1)$ and $4f^2-2f-1$ is 1, we deduce that we can take $D(f)$ one of $(f-1)(2f+1)$, $2f^2-1$, $4f^2-2f-1$ or

$$D(f) = 3, 5, 7, 9, 11, 15, 21, 23, 25, 27, 45.$$

It is now easy to verify directly that $D(f) = (f-1)(2f+1)$, $2f^2-1$, $4f^2-2f-1$ give the solutions listed as (II, Ai), (II, Aii), (II, Aiii) in Table 2.

Relation $x^f y^{-1} = 1$.
If we use the relation $U_{18} = U_k$ we obtain the following possibilities:

$$D(f) = 3, 5, 7, 9, 11, 15, 23;$$
$$D(f) = 2f-1,\ 3(2f-1),\ f^2+f-1,\ 2f^2-1,\ (f+1)(2f-1).$$

If we use the relation $U_5 = U_k$ we obtain the following possibilities:

$$D(f) = 3, 5, 7, 9, 11, 21, 23, 27, 73;$$
$$D(f) = f+1,\ 3(f+1),\ 5(f+1),\ 2f-1,\ f^2+f-1,$$
$$3\big(f^2+f-1\big),\ 5\big(f^2+f-1\big),\ 2f^2-1,\ (f+1)(2f-1).$$

Any $D(f)$ must divide some possibility in each of these two groups. Since the resultants of $2f-1$ with $f+1$, f^2+f-1, and $2f^2-1$ are 3, -1, and -2, we deduce that we can take $D(f)$ one of f^2+f-1, $2f^2-1$, $(f+1)(2f-1)$ or

$$D(f) = 3, 5, 7, 9, 11, 15, 21, 23, 27, 45, 73.$$

It is now easy to verify directly that $D(f) = f^2+f-1$, $2f^2-1$, $(f+1)\times(2f-1)$ give the solutions listed as (II, Aiv), (II, Av), (II, Avi) in Table 2.

Relation $x^{-2f^2} y^{1+2f} = 1$.
If we use the relation $U_1 = U_k$ we obtain the following possibilities:

$$D(f) = 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 29, 53, 59, 107;$$
$$D(f) = 2f^2-1,\ 2f^3-1,\ 2f^3+f^2-1,\ 4f^3-1,\ 4f^3-f-1.$$

The last line gives the solutions listed as (II, Avii), (II, Aviii), (II, Aix), (II, Ax), (II, Axi) in Table 2.

The Mathematica program "refineAII.sastry" analyzes the various possibilities for a finite $D(f)$, rejecting those which appear as a specialization of (II, Ai) to (II, Axi). This reduces the list to:

Relation $x^{-1+2f}y^{-2}=1$:

$$D(f)=3, \qquad f=2, \qquad k_0=\mathbb{F}_{2^2};$$
$$D(f)=11, \qquad f=2^7, \qquad k_0=\mathbb{F}_{2^{10}}.$$

Relation $x^f y^{-1}=1$:

$$D(f)=3, \qquad f=2, \qquad k_0=\mathbb{F}_{2^2};$$
$$D(f)=11, \qquad f=2^2, \qquad k_0=\mathbb{F}_{2^{10}}.$$

Relation $x^{-2f^2}y^{1+2f}=1$:

$$D(f)=7, \qquad f=1, \qquad k_0=\mathbb{F}_{2^3};$$
$$D(f)=7, \qquad f=2^2, \qquad k_0=\mathbb{F}_{2^3}.$$

These possibility do occur and correspond to types (II, Axii)–(II, Axvii) in Table 2.

This completes the analysis of Case AII.

12. Comments on the computer programs

Several Mathematica programs were used to complete the calculations.

The first program "header.sastry" consists of a header file and the program solveB.sastry for eliminating equation $(3m)$. The header file contains the following functions:

RemovePairs[U]. The input is a list U and the function returns a list of all elements of U which appear with odd multiplicity, i.e. removes all pairs of equal elements of U.

EqualPairs[U]. The input is a list U and the function returns 1 if all elements appear with even multiplicity, and 0 otherwise. It is faster than checking whether RemovePairs[U] is the empty list or not, and is used to deal with the numerical cases at the end.

lcm[U] and gcd[U] return the least common multiple and the greatest common divisor of a list of integers.

Red[U, d]. This function takes a list U of polynomials in one variable f, reduces it modulo another polynomial d and returns it after removing all pairs of equal elements. The reduction is done after multiplication by a suitable integer so to ensure that the elements of the reduced list have degree less than the degree of d.

RedDeg[U, d]. This function starts with a list U of polynomials modulo d and, assuming that the list splits into equal pairs modulo d, attempts to obtain a complete set of moduli e for which d must belong to this set. The

method proceeds by means of a tree search as follows. The first element U_1 of the list must be equal to some other element U_k of the list. We set aside the value $e = U_1 - U_k$, and note that if $d \neq 0$ then U must consist of equal pairs for a new modulus which is the semi-resultant of d and e. If this is equal to e or a constant, we put it into our list of possibilities, otherwise we call RedDeg$[U, e]$ recursively.

In practice, this method leads to too large a list of possibilities with a constant value of e, and this set is trimmed by means of a function CompCheck[ ], which considers directly, for all $f = 2^i$ in a finite field, whether the list U can be composed of equal pairs modulo d and modulo some divisor of the constant e. If a divisor e' of e is found for which this cannot happen then we can replace e by e/e' and repeat the procedure.

The header file also contains the initialization of the vector of exponents of M_i and N_j, after elimination of Eqs. (1) and (2I) or (2II).

The programs in question use standard Mathematica functions and the functions in the header file. They ran at various times on Sun and Silicon Graphics workstations at the Institute for Advanced Study in Princeton, New Jersey, and at the Eidgenössische Technische Hochschule in Zürich, Switzerland. They are available on request from the author.

Acknowledgment

The author wishes to thank the Eidgenössische Technische Hochschule in Zürich, Switzerland, for providing financial support during the preparation of this paper.

References

[B] E. Bombieri, Thompson's problem ($\sigma^2 = 3$), Invent. Math. 58 (1980) 77–100.

[E] M. Enguehard, Caractérisation des groupes de Ree. Révision dans les gropes finis. Groupes du type de Lie de rang 1, Astérisque 142–143 (1986) 49–139, 296.

[S] N.S.N. Sastry, Large uniqueness, up to conjugacy, of the finite Ree and Suzuki simple groups in the defining group of Lie type, Preprint, 1995.

[T] J.G. Thompson, Toward a characterization of $E_2^*(q)$, Part I: J. Algebra 7 (1967) 406–414, Part II: J. Algebra 20 (1972) 610–621, Part III: J. Algebra 49 (1977) 162–166.